"D1" on 409

spec. p.2

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00

A1

(11) International Publication Number: WO 97/03397

(43) International Publication Date: 30 January 1997 (30.01.97)

(21) International Application Number: PCT/EP96/02999

(22) International Filing Date: 9 July 1996 (09.07.96)

(30) Priority Data:
9502537-5 10 July 1995 (10.07.95) SE

(71) Applicant *(for all designated States except US)*: BENKTA CONSULTING AB [SE/SE]; Bengt Andersson, Skogshällsbacken 1, S-163 58 Spånga (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ANDERSSON, Bengt [SE/SE]; Skogshällsbacken 1, S-163 58 Spånga (SE). GILLISPIE, William, W. [US/SE]; Nötskrikevägen 30, S-134 42 Gustavsberg (SE).

(74) Agents: ASKERBERG, Fredrik et al.; L A Groth & Co. KB, P.O. Box 6107, S-102 32 Stockholm (SE).

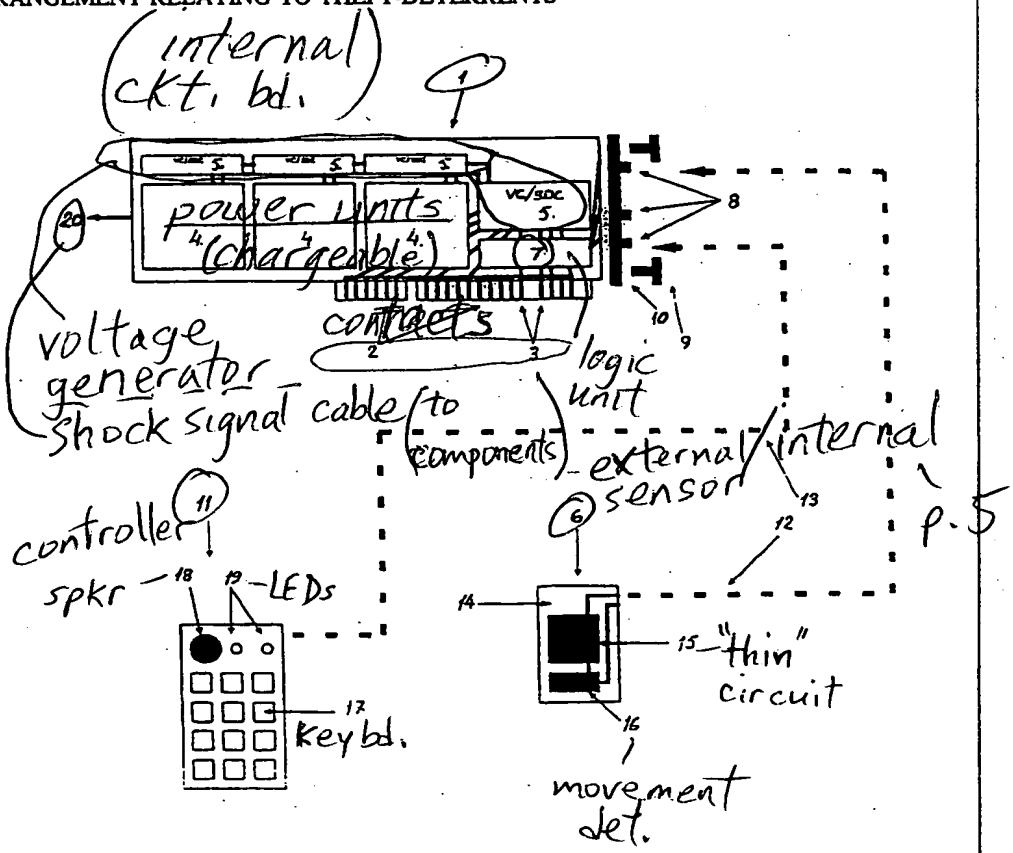
(81) Designated States: BR, CA, CN, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD AND AN ARRANGEMENT RELATING TO THEFT-DETERRENTS

(57) Abstract

In a method and an arrangement for deterring the theft of computers or vital computer components, an internal logic unit (7) is used to trigger a shock signal when the computer is subjected to improper manipulation. The logic unit (7) is connected electrically to external sensors (6) which include thin electric circuits (15) and movement detectors (16) such as to sense/detect improper manipulation of computer components or the computer itself. The arrangement can be controlled and monitored by a code panel (11). The code panel (11) includes a keyboard (17), a loudspeaker (18) and light-emitting diodes (19). The shock signal is directed to one or more vital components of the computer, these components being destroyed by the shock signal when triggered.



p.5

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

A METHOD AND AN ARRANGEMENT RELATING TO THEFT-DETERRENTS

TECHNICAL FIELD

The present invention relates to a method and to a security arrangement for deterring the theft of computers or parts thereof. The security arrangement includes a protective device having one or more external sensors.

DESCRIPTION OF THE BACKGROUND ART

Many different solutions and concepts have been proposed with respect to protection against theft of computers, and then particularly personal computers, which have become a theft attractive item and are often easy to steal from work places and schools. These proposed solutions have included the use of simple mechanical devices, such as screwing the computer to the computer table for instance. Attempts have also been made to prevent manipulation of computers with the aid of different key and code arrangements with the intention of preventing the computer from being started-up and operated. Means for guarding against the improper or unauthorized use of software are also known to the art.

However, none of the hitherto proposed solutions and concepts directed towards protecting theft-attractive computers has been found effective. Present-day thieves do not often steal the entire computer, but solely the vital or expensive components therefrom. There is no effective means against such theft.

SUMMARY OF THE INVENTION

The present invention alleviates this situation by providing a safety or security arrangement which is characterized in that the external sensor or sensors included in the protective device is/are activated by improper actuation of

the computer and each of which is connected to a generator means. Upon receipt of a signal from at least one of the sensors, the generator means functions to direct a shock signal to one or more of the vital or expensive computer components so as to partially or completely destroy said components. Because the computer components (at least those considered valuable to a thief) are destroyed, the theft of or the misappropriation of the computer will no longer be attractive to a thief.

The shock signal is preferably comprised of a series of high-voltage electrostatic or electromagnetic pulses or spikes which are triggered as a result of activating at least one of the sensors. A sensor can be triggered in result of unwarranted or improper movement of the computer, inactivation of the computer voltage supply and/or improper opening of the computer casing.

Because the security arrangement shall be active even when the computer is inactive, the protective device includes a separate chargeable power unit which is intended to be charged when the computer is switched on and which enables the shock signal to be generated even when the computer is switched off, without the computer memory or processing facility being used. The power unit is connected to voltage converting and shock-signal generating circuits which are also connected to an internal logic unit and to an interface for the external sensors and a code panel.

In order to avoid triggering of the shock signal in the event of proper or qualified actuation of a sensor, for instance when servicing the computer, the security arrangement function can be disconnected by means of a code signal. This is preferably effected through the medium of a code panel having a keyboard or keypad through which the code signal can be entered.

DESCRIPTION OF PREFERRED EMBODIMENTS

The inventive security arrangement will now be described in more detail with reference to a preferred embodiment thereof and also with reference to the accompanying drawing.

The drawing illustrates the principle features of a preferred embodiment of the inventive security arrangement in the form of an internal circuit board 1 which is connected to a series of electrical circuit board contacts 2 provided in the computer (not shown) to be protected against theft. The circuit board contacts 2 are connected electrically to the expansion bus of the computer mother board. When the computer operates normally, electric current is supplied to the circuit board 1 through current supply contacts 3.

The circuit board 1 has mounted thereon an appropriate number of chargeable power units 4 (batteries, capacitors or the like) which are supplied form the supply contacts 3 when the computer is in normal operation. The power units 4 are connected electrically to voltage converting and generator means 5 (VC/SDC) for generating a shock voltage signal when a triggering signal is obtained from one or more of the external sensors 6 described below. The shock signal is generated as a controlled series of pulses being conducted directly to the target components through a shock signal cable 20. The signal is returned through the expansion bus on the computer mother card back to an internal logic unit 7 via the circuit contacts 2 and the return line(s) of the computer bus on the mother card. The computer components, such as the mother card, the processor and/or the main memory, to be destroyed as a whole or partly are connected to the shock signal cable 20 by jumping gaps (not shown) transferring only the shock signal comprising a series of high-voltage electromagnetic pulses or spikes.

The shock signal cable 20 may be one single line branched off

switch?

for each one of the computer components selected to be destroyed. Another embodiment may comprise separate shock signal cable lines connected between the circuit board 1 and the computer components selected to be destroyde.

The circuit board 1 is connected to a series of external contacts 8 on the outside of the computer via an interface included in the internal logic unit 7. The series of contacts 8 are fastened in a conventional manner with the aid of locking screws 9 through the medium of an attachment plate 10. The contacts 8 are used partly to connect one or more external sensors 6 and partly to connect a code panel 11. Connection of the sensors 6 and the code panel 11 is illustrated by electric conductors 12 and 13 respectively. The conductors 12, 13, or cables, are electrically screened and strengthened with regard to mechanical strength.

Each sensor 6 includes a plate 14 having an adhesive film coating on at least one side thereof. The film incorporates a thin electrically conductive circuit 15. The plate 14 also carries a movement detector 16.

A sensor 6 can be used in a number of different ways. For instance, it may comprise a wall anchor plate, i.e. can be securely mounted on a wall of the room in which the computer is used and is situated close to the computer. The film containing circuit 15 is fastened to the wall and if a thief cuts the wire or cable 12 leading to the computer so as to free the computer from the wall anchor, this will be sensed by the internal logic unit 7 and a shock signal will be triggered as a result. Even though the sensor 6 should be removed carefully from the wall while leaving the wire or cable 12 undisturbed, this will nevertheless be sensed by the internal logic unit 7, by virtue of the fact that the circuit 15 incorporated in the film will be torn to pieces when the adhesive film is released, and also by virtue of actuation of the movement detector 16. Should the thief simply rip the

entire wall anchor from the wall, this will be detected by the movement detector 16 and the logic unit 7 will thereby be activated to trigger the shock signal.

Correspondingly, the sensor 6 can be disposed as an insert between the underside of the computer and the table surface on which the computer stands. Lifting of the computer will actuate the movement detector 16 of the sensor 6 with the aforesaid result. Cutting of the wire or cable 12 will also cause the shock signal to be triggered.

The sensor 6 may also be applied to the outside or the inside of the computer casing, so as to activate the internal logic unit 7 should an attempt be made to remove the casing from the computer in order to reach significant or expensive components in the computer.

An attempt to release the internal circuit board 1 from its contacts 2, 3 will also activate the internal logic unit 7 so as to trigger the shock signal. The same applies with regard to an attempt to release the external lock plate 10 from the computer. In this case, the internal logic unit 7 will detect the breakage of the wires 12 to the external sensors 6, for instance by sending electric interrogation pulses from the internal logic unit 7 to the sensors 6.

As before indicated, the security arrangement is activated and deactivated by means of the code panel 11. This panel includes a device in the form of a remote control box provided with a keyboard 17 for keying code signals into the internal logic unit 7 of the security arrangement. Thus, the security arrangement can be activated and deactivated through the keyboard 17. It is also possible to interrupt accidental triggering of the shock signal, by entering a set code through the keyboard 17, when the shock signal is not triggered in real terms until a predetermined time period has lapsed after activation of the internal logic unit by a

sensor 6. A loudspeaker 18 and/or light-emitting diodes (LED) 19 arranged on the code panel 11 function to issue acoustic and/or light warning signals to the effect that the internal logic unit 7 has been activated and that a shock signal that will destroy vital parts of the computer will be triggered after said predetermined time period.

In the event of the circuit (cable 13) extending between the internal logic unit 7 and the code panel 11 being broken, so as to make it impossible to reset/deactivate a triggered shock signal with the aid of the code panel 11, the invention provides the convenient following alternative. The imminent but time-delayed triggering of the shock signal (caused for instance by breaking the aforesaid circuit) can be nullified by manipulating the mains voltage supply switch in a predetermined off/on or on/off sequence. This predetermined "failsafe" sequence is incorporated in the logic unit 7 and is unique for each security arrangement supplied. For instance, the sequence can be based on the selection of a given number of off/on (or on/off) switch manipulations per unit of time. For instance, the sequence may necessitate maneuvering the mains switch off/on six times during a period of three minutes with the following sequence of intermediate periods:

Intermediate period I	(on 1 - off 2):	20 seconds
Intermediate period II	(off 2 - on 3):	30 seconds
Intermediate period III	(on 3 - off 4):	40 seconds
Intermediate period IV	(off 4 - on 5):	40 seconds
Intermediate period V	(on 5 - off 6):	50 seconds

The total intermediate time period = one time unit = 180 sec., i.e. 3 min. Naturally, the number of times the switch is switched on/off or off/on is optional, as is also the duration of the total time unit and the duration of respective intermediate periods.

The loudspeaker 18, the light-emitting diodes 19 and the keyboard 17 on the code panel 11 can also be used for other messages from and to the internal logic unit 7. For instance, the diodes 19 may continuously show the status of the security arrangement.

It will be evident from the aforegoing that a computer equipped with an inventive security arrangement will make a computer useless in response to improper interference with the computer or parts thereof, by triggering a shock signal when the computer casing is improperly open and/or when the computer is improperly, or unlawfully, removed from its normal working position. The shock signal will destroy valuable components of the computer and also generate an alarm. Improper attempts to inactivate and/or circumvent the security arrangement will result in permanent destruction of the vital electronic components of the computer (for instance its memory, the central processor unit (CPU), the mother card and the like). This destruction is thus achieved by a series, preferably a controlled series, of high-voltage electrostatic or electromagnetic pulses delivered via the data circuits and electrical supply circuits of the computer.

Although the invention has been described and illustrated with reference to a preferred exemplifying embodiment thereof, the person skilled in this art will realize that different modifications and further developments are conceivable without departing from the inventive concept. E.g. jumping gaps may be replaced with appropriate electronic components like capacitors. The invention is therefore not restricted to the aforedescribed and illustrated embodiments, and is solely restricted by the scope of the following Claims.

CLAIMS

1. A method of deterring the theft of computers and the like by detecting improper or unlawful interference of a computer with the aid of one or more sensors (6), said method being **characterized** in that when activated said one or more sensors (6) cause a generator means (5) to trigger a shock signal that is directed towards one or more vital or expensive target computer components such as to partially or completely destroy said components.

2. A method according to Claim 1, **characterized** by periodic interrogation of the sensors (6) with the aid of electric pulses delivered from an internal logic unit (7).

3. A method according to Claim 1 or 2, characterized in that said shock signals are a controled series of pulses directed to said vital or expensive target computer components.

4. A method according to Claim 1 or 3, characterized in that said vital or expensive target computer components are one or more of the mother card, the processor and main memory or parts thereof included in the computer.

5. A method according to any one of the preceding Claims, **characterized** by triggering the shock signal first after a predetermined time period has lapsed after actuation of the generator means (5).

6. A security arrangement for deterring the theft of computers and the like and comprising a protective device having one or more external sensors (6), said security arrangement being **characterized** in that said sensors (6) are activatable by improper manipulation of the computer, and in that each one of said sensors (6) is connected to a generator means (5) which, in response to receiving a signal from at

least one of the sensors (6), functions to produce a shock signal which is directed to one or more vital or expensive target computer components so as to partially or completely destroy said components.

7. A security arrangement according to Claim 6, **characterized** in that the shock signal comprises a series of high-voltage electrostatic or electromagnetic pulses.

8. A security arrangement according to Claim 6 or Claim 7, **characterized** in that respective sensors (6) are activatable in response to improper movement of the computer, inactivation of the computer voltage supply and/or improper opening of the computer casing.

9. An arrangement according to any one of Claims 6-8, **characterized** in that the protective device includes a separate chargeable power unit (4) which is intended to be charged when the computer is switched-on and which also enables the generation of said chock signal when the computer is switched-off without the computer memory or processing capacity of the computer being used.

10. An arrangement according to Claim 9, **characterized** in that the power unit (4) is connected to voltage conversion and shock-signal generator circuits (5) which are also connected to an internal logic unit (7) and to interfaces for the external sensors (6) and a code panel (11).

11. An arrangement according to any one of the Claims 6-10, **characterized** in that the shock signal is generated as a controlled series of pulses conducted directly to the target computer components through a shock signal cable (20) connected to the target computer components by one or more jumping gaps, the return circuitry being set up by the ordinary computer bus (via 2) of the computer mother card.

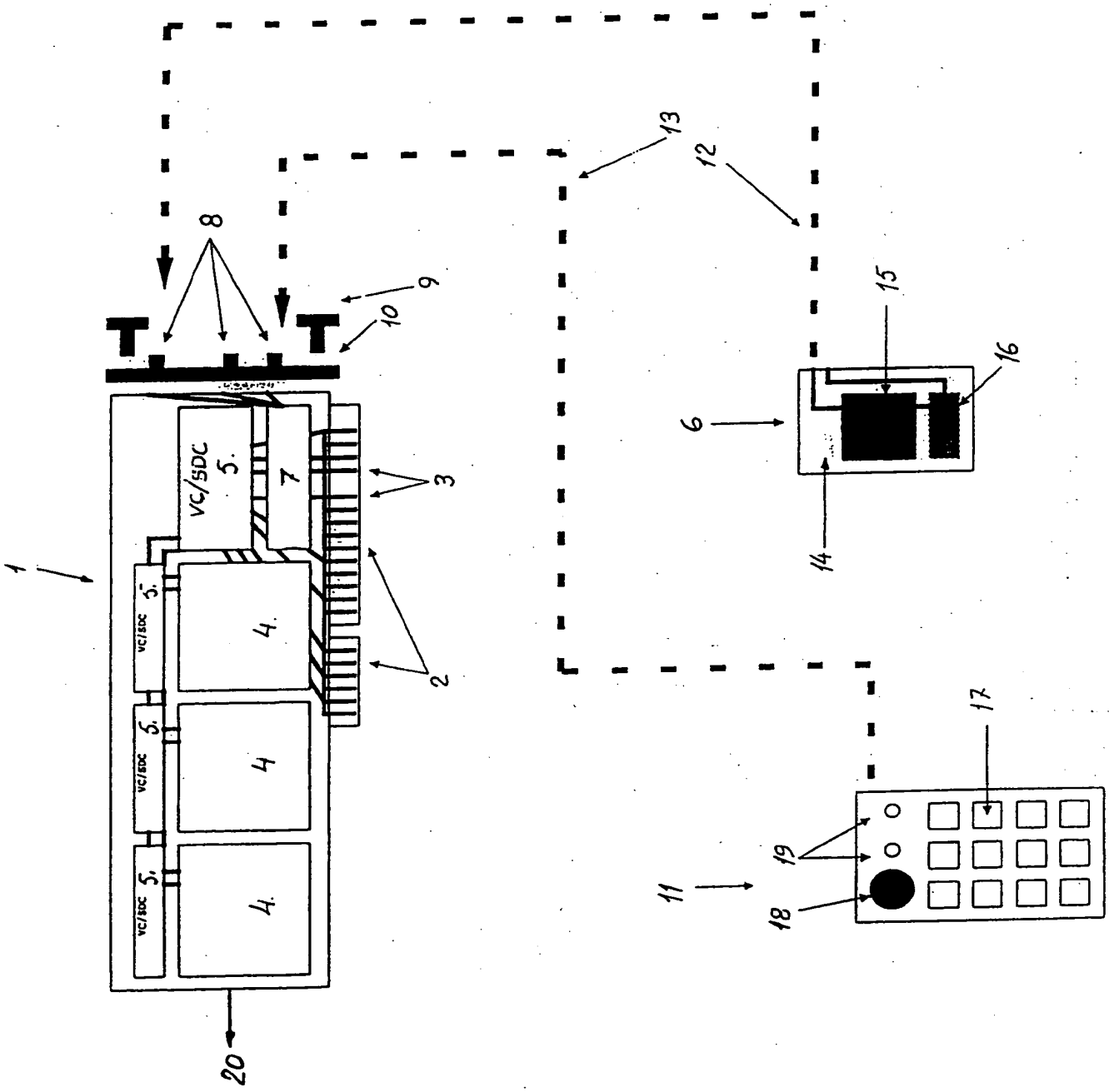
12. An arrangement according to Claim 8 and Claim 10, characterized in that each of the external sensors (6) comprises a plate-like means (14) whose at least one surface has applied thereon an adhesive film which incorporates a thin electrically conductive circuit (15) and a movement detector (16), wherein the sensor (6) when mounted on a wall or on the outside of the computer, preferably on the underside thereof, or against the inside of the computer lid, is activated to deliver a signal to the generator means (5) when the sensor (6) is removed from the wall, separated from the computer by lifting the computer, separated from the lid as the lid is opened and/or when the sensor (6) is moved together with the computer.

13. An arrangement according to Claim 10, **characterized** in that the code panel (11) has the form of a remote control unit provided with keys (17), wherein the security arrangement can be activated and inactivated preferably by keying-in predetermined codes through the keys (17).

14. An arrangement according to Claim 13, characterized in that the code panel (11) includes a series of light-emitting diodes (19) for displaying the operational status of the computer and/or a loudspeaker (18) for generating a series of high-frequency acoustic signals to draw attention to a malfunction and/or a theft attempt.

15. An arrangement according to any one of Claims 9-11, **characterized** in that the power unit (4), the voltage conversion and shock signal generating circuits (5), and the internal logic unit (7) are arranged on a circuit board (1) which can be connected via internal circuit board contacts (2, 3) to the computer expansion bus on the computer mother card, and which are connected to an external lock plate (10) having sensor contacts (8) for the external sensors (6), wherewith a breakage between the circuit board (1) and the circuit board contacts (2, 3) or the sensor contacts (8)

results in a shock signal from the generator means (5) fed through the shock signal cable (20) to said selected target computer components.


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
VC/SDC

INTERNATIONAL SEARCH REPORT

Inter. nal Application No
PCT/EP 96/02999

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,5 406 261 (GLENN JAMES T) 11 April 1995 see abstract; figures 6,7	1,4-8
Y	see column 2, line 1 - column 3, line 65	2,9,12, 14
A	---	13
Y	US,A,4 783 801 (KAULE WITTICH) 8 November 1988 see abstract	2

Y	US,A,4 218 763 (BRAILSFORD LAWRENCE J ET AL) 19 August 1980 see abstract; figure 1 see column 3, line 33 - line 61 see column 11, line 11 - line 15	9,14
A	---	6
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 November 1996	16. 12. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 96/02999

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	GB,A,2 182 467 (NCR CO) 13 May 1987 see abstract; figures 3,13,14 see page 5, line 106 - line 125	12
A	WO,A,91 05306 (UNIV SYDNEY TECH ;CRADLE ELECTRONICS (AU)) 18 April 1991 see abstract; figure 2 see page 4, paragraph 2 - paragraph 3	10,11

1

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter. nal Application No
PCT/EP 96/02999

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-5406261	11-04-95	NONE		
US-A-4783801	08-11-88	DE-A-	3347483	11-07-85
		EP-A-	0151714	21-08-85
		JP-A-	60157648	17-08-85
US-A-4218763	19-08-80	NONE		
GB-A-2182467	13-05-87	CA-A-	1265244	30-01-90
		DE-A-	3635938	07-05-87
		FR-A-	2589602	07-05-87
		JP-A-	62117047	28-05-87
		US-A-	4691350	01-09-87
WO-A-9105306	18-04-91	AU-B-	645503	20-01-94
		AU-A-	6503490	28-04-91
		CA-A-	2067331	04-04-91
		EP-A-	0494913	22-07-92
		IL-A-	95903	31-08-95
		US-A-	5353350	04-10-94